Swingvy HR hub, Payroll and Benefits Platform v2.1.29 Security Target

Common Criteria: EAL2

Document version: 1.1

Document date: 21-JULY-2020

Prepared By

Securelytics

www.securelytics.my

Document management

Document identification

Document title	Swingvy HR Hub, Payroll and Benefits platforms v2.1.29 Security Target
Document version	1.1
Document date	21-JULY-2020
Author	Muzamir Mohamad
Release Authority	Swingvy

Document history

Version	Date	Description
0.1	15-JUL-2018	Released for internal review
0.2	15-AUG-2018	Released to evaluators
0.3	1-SEPT-2018	Updated Section 6
0.4	16-NOV-2018	Updated Section 1 until 6 to address several issues raised by the evaluator in MySEF-3-EXE-E048-EOR1-d1
0.5	10-JAN-2019	Updated Section 1 until 6 to address several issues raised by the evaluator in MySEF-3-EXE-E048-EOR2-d1
0.6	03-JUNE-2019	Updated Section 1 to address several issues raised by the evaluator in MySEF-3-EXE-E048-EOR6-d1
0.7	28-APR-2020	Updated Section 1.2, Section 3.4, Section 4.3 and Section 4.4 to address several issues raised by the evaluator in MySEF-3-EXE-E048-EOR7-d1
0.8	15-MAY-2020	Updated TOE version number raised by the evaluator in MySEF-3-EXE-E048-EOR7-d2
1.0	1-JUNE-2020	Final Release
1.1	21-JULY-2020	Updated Section 5.2

Table of Contents

1 Security Target introduction

1.1 ST reference

ST Title	Swingvy HR Hub, Payroll and Benefits platforms v2.1.29 Security Target
ST Version	1.1
ST Date	21-JULY-2020

1.2 TOE reference

TOE Title	Swingvy HR Hub, Payroll and Benefits platform
TOE Version	2.1.29

1.3 Document organization

This document is organized into the following major sections:

- Section 1 provides the introductory material for the ST as well as the TOE description (ASE_INT.1).
- Section 2 provides the conformance claims for the evaluation (ASE_CCL.1).
- Section 3 provides the definition of the security problem that the TOE has been designed to address (ASE_SPD.1).
- Section 4 defines the security objectives for the TOE and the environment (ASE_OBJ.2).
- Section 5 contains the security functional and assurance requirements derived from the Common Criteria, Part 2 and 3 respectively, which are in turn satisfied by the TOE and the development lifecycle (ASE_REQ.2).
- Section 6 provides a summary of the TOE specification, identifying the IT security functions provided by the TOE (ASE_TSS.1).

1.4 Defined terms

The following table defines all subjects, objects, operations, security attributes, external entities and other key terms that are used within the statements of security functional and assurance requirements. It also describes the acronym used in this documentation.

Term	Description
Authentication Data	It is information used to verify the claimed identity of a user.
ACL	Access control lists
Admin	The Admin is a pre-set user within the TOE that is created during TOE installation. All functions assigned to Admin are added new user profile and roles, edit/change and delete existing user profile and role setting, cancelling the form changes, closing the form, change password, and security setting
TSF data	Data created by and for the TOE, which might affect the operation of the TOE.
TSC	TOE Scope of Control, the set of interactions that can occur with or within a TOE and are subject to the rules of the TSP
TSP	TOE Security Policy, a set of rules that regulate how assets are managed, protected and distributed.
Unauthorised user	An unauthorised user is a user that does not have authorisation to use the functionality of the TOE.
User / TOE User	Users/TOE Users are Admins and Authorised Users
User data	Data created by and for the user, which does not affect the operation of the TSF.

1.5 TOE overview

1.5.1 TOE usage and major security functions

The TOE is a software as a Service (SaaS) whilst installed, configured and deployed in the cloud platform services (PaaS). The TOE operates in Multi-Tenant Mode that provide solutions for managing and operating Human Resource, Payroll and Benefits. TOE is accessible via a web browser from mobile devices and PCs.

Below are the primary features of the TOE:

- HR Information System (HRIS) - provides employee management, leave management and employee talent management.
- Payroll - automatically calculates all government required tax calculations and provides automated payroll service to the users, specifically admins of companies.
- Benefits store - allows admins to purchase benefits (such as group insurance) for their employees.

The following table highlights the range of security functions implemented by the TOE.

Security function	Description
Access control	The TOE manages access control within each organisation based on user IDs, user roles and access control lists. Each ACL maps users and roles to the operations that they are permitted to perform on the object.
Identification and authentication	The TOE requires that each user is successfully identified (user IDs) and authenticated (Minimum password length of 8-characters with at least 1 capital letter and 1 special or numeric character) before any interaction with protected resources is permitted.
Security Management	The TOE provides functions that allow management of the TOE and its security functions. The TOE restricts access to the management functions based on the role of the user.

1.5.2 TOE Type

The TOE type is a web-based application, in which the TOE is a SaaS designed to be used for a web-based application environment. The TOE provides security functionality such as access control, identification and authentication and security management

1.5.3 Supporting Hardware, software and/or firmware

The underlying hardware and software that is used to support the TOE are:

Minimum System Requirements	
Operational Environment (configured, installed and deployed on PaaS)	
Operating Systems	Centos 7
Processor	x86/x64 architecture
Memory (RAM)	1 GB
Software	Swingvy v2.1
Database (RDBMS)	MySQL 5.7
Supporting software	Java 8
End-user	
Web Browser	• Chrome 35 • Safari 10 • Firefox (Latest version) • Microsoft Edge • Microsoft Internet Explorer 11
PC System Requirements	• OS X 10.10 • Windows 7 or higher

1.5.4 Excluded From the TOE

The only security functionality addressed by the evaluation is the functionality specified by the functional requirements in Section 5.2, and does not include additional platform such mobile application. The following items are out of the scope of the evaluation:

- Mobile Application platform

1.6 TOE description

1.6.1 Physical scope of the TOE

The TOE is web application hosted on enterprise cloud environment. Therefore, the TOE itself has no physical boundaries. A typical implementation of the TOE can be found in Figure 1 below, which identifies the various components of the TOE architecture. In order for the TOE users to access the TOE features such as HR Information System (HRIS), Payroll and Benefit Store, TOE users need to browse to https://www.swingvy.com.

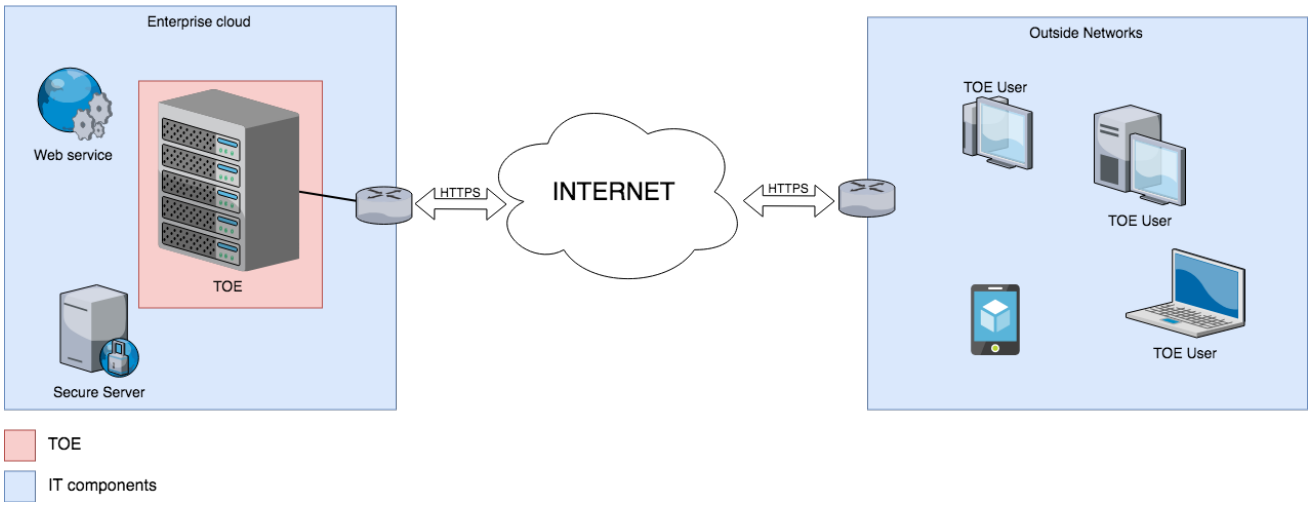

Figure 1 – TOE

1.6.2 Logical scope of the TOE

The logical boundary of the TOE is summarized below.

a) **Access Control.** The access control function permits a user to access a protected resource only if the user ID or user role has permission to perform the requested action on the resource. Access rules are stored in Access Control Lists associated with each object in the TSC. The TOE maintains role-based access control mechanisms to ensure that the TOE security management functions are restricted to those who have the privilege to access them. Admin user is the only user that has the ability to assign privilege to each individual Authorised User.

b) **Identification & Authentication.** All users are required to be identified and authenticated before any information flows are permitted. At the login page, TOE users need to key in a valid username and password in order to access the TOE. The acceptable minimum password length is 8-characters with at least 1 capital letter and 1 special or numeric character. The TOE checks the credentials presented by the user against the authentication information stored in the database.

c) **Security Management.** The TOE contains various management functions to ensure efficient and secure management of the TOE. The TOE restricts access to the management functions

based on the role of the user. The TOE defines two security management roles: Admin and Authorised User.

Admin user able to perform:

- User Management: Add User, View/Edit User Profile and Terminate User
- Group Management: Add/Edit/Delete Group, Edit User Permission Group, Edit User Group
- Organisation: Add/Edit/Delete Job Title
- Organisation: Add/Edit/Delete Department
- Leave Management
- Talent Management
- Payroll Management
- Benefits Store: Health Benefit Management
- Edit Office and Time zone setting
- Change password for own account

Authorised User able to perform:

- User Management: View/Edit User Profile
- Leave Management
- Change password for own account

2 Conformance Claim

The ST and TOE are conformant to version 3.1 (REV 5) of the Common Criteria for Information Technology Security Evaluation.

The following conformance claims are made for the TOE and ST:

- **Part 2 conformant.** Conformant with Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, version 3.1 (REV 5), April 2017
- **Part 3 conformant, EAL2.** Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1 (REV 5), April 2017. The assurance level for this evaluation is Evaluation Assurance Level 2 (EAL2)

3 Security problem definition

3.1 Overview

This section describes the nature of the security problem that the TOE is designed to address. The security problem is described through:

a) a series of ***threats*** that the TOE has been designed to mitigate,

b) specific ***assumptions*** about the security aspects of the environment (both IT related and non-IT related elements) in which the TOE will operate, and

c) any relevant ***organisational security policies*** statements that are made in terms of rules or guidelines that must be followed by the TOE and/or the operational environment.

3.2 Threats

The TOE addresses the following threats:

Identifier	Threat statement
T.WEB_ATTACK	An unauthorized person may attempt to compromise the integrity, availability and confidentiality of enterprise information by performing web application attacks.
T.NOMGMT	An unauthorized person modifies management data that they are not authorised to access resulting in a loss of integrity of the data that the TOE uses to enforce the security functions.
T.UNAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
T.PSWD_CRACKING	An unauthorized person may take advantage of weak administrative passwords to gain privileged access to the TOE functions.

3.3 Organisational security policies

No organisational security policies have been defined regarding the use of the TOE.

3.4 Assumptions

The following specific conditions are assumed to exist in an environment where the TOE is employed.

Identifier	Assumption statement
A.NOEVIL	It is assumed that the person who manages the TOE is not hostile and is competent.
A.NOTRST	The TOE can only be accessed by authorized users.
A.COMM_PROTECT	The IT environment will provide a secure channel so that all potentially valuable information (including credentials and enterprise data) is protected between the user and application server
A.CLOUD	The cloud environment will provide a load balancing, web application firewall (WAF) and network traffic filters (e.g. access control lists (ACL)) services in order to prevent the attacker from performing any malicious activity against the TOE and to prevent application failure

4 Security objectives

4.1 Overview

The security objectives are a concise statement of the intended response to the security problem defined in Section 3. They are security objectives for the TOE to address and additional objectives that provide specific direction for the intended environment in which the TOE is to operate.

4.2 Security objectives for the TOE

Identifier	Objective statements
O.ACC_CTRL	The TOE shall ensure that only authenticated and authorized users can access the TOE functionality and protected application resources.
O.AUTH	The TOE must provide measures to uniquely identify and authenticate users prior to granting access to the functions or resources protected by the TOE.
O.MANAGE	The TOE must allow TOE Admin to effectively manage the TOE and users, while ensuring that appropriate controls are maintained over those functions.
O.PASSWORD	The TOE must ensure that the TOE user password has a minimum password length of 8-characters with at least 1 capital letter and 1 special or numeric character.

4.3 Security objectives for the environment

Identifier	Objective statements
OE.ADMIN	The owners of the TOE must ensure that the Admin who manages the TOE is not hostile and is competent.
OE.AUTHDATA	Those responsible for the TOE must ensure that all access credentials, such as passwords or other authentication information, are protected by the users
OE.COMM_PROTECT	The IT environment shall provide the server-side of a secure channel so that all potentially valuable information (including credentials and data) is protected between the user and application.
OE.CLOUD	The cloud environment shall provide load balancing, web application firewall (WAF) and network traffic filters (e.g. access control lists (ACL)) services so that the TOE is protected from any malicious activity and application failure

4.4 Security objectives rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions and threats.

OBJECTIVES \ THREATS/ ASSUMPTIONS	T.WEB_ATTACK	T.NOMGMT	T.UNAUTH	T.PSWD_CRACKING	A.NOEVIL	A.NOTRST	A.COMM_PROTECT	A.CLOUD
O.ACC_CTRL	✔	✔	✔					
O.AUTH		✔	✔					
O.MANAGE		✔						
O. PASSWORD				✔				
OE. ADMIN					✔			
OE.AUTHDATA			✔			✔		
OE.COMM_PROTECT							✔	
OE.CLOUD								✔

4.4.1 TOE security objectives rationale

The following table demonstrates that all security objectives for the TOE are trace back to the threats in the security problem definition.

Threats/OSPs	Objectives	Rationale
T.WEB_ATTACK	O. ACC_CTRL	The objective ensures that only authenticated and authorized users can access the TOE functionality and protected application resources.
T.NOMGMT	O.ACC_CTRL	The objective ensures that the TOE identifies and authenticates all users before they access a protected resources or functions.
	O.MANAGE	This objective ensures that the TOE provides the tools necessary for the authorized admin to manage the security-related functions and that those tools are usable only by users with appropriate authorizations.

Threats/OSPs	Objectives	Rationale
	O.AUTH	The objective ensures that the TOE restricts access to the TOE objects to the authorized users
T.UNAUTH	O.ACC_CTRL	The objective ensures that the TOE restricts access to the TOE objects to the authorized users.
	O.AUTH	The objective ensures that the TOE identifies and authenticates all users before they access a protected resources or functions.
	OE.AUTHDATA	The TOE must ensure to uniquely identify and authenticate users prior to granting access to the functions or resources protected by the TOE.
T.PSWD_CRACKING	O.PASSWORD	The TOE must ensure that all users adhere with the acceptable password policy to avoid from unauthorised user taking advantage of weak password and gain unauthorised access to the TOE functions.

4.4.2 Environment security objectives rationale

The following table demonstrates that all security objectives for the operational environment are trace back to assumptions in the security problem definition.

Assumptions	Objective	Rationale
A.NOEVIL	OE.ADMIN	This objective ensures that those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.
A.NOTRST	OE.AUTHDATA	This objective ensures that only authorised user able to access the TOE and all access credentials, such as passwords or other authentication information are protected by that users
A.COMM_PROTECT	OE.COMM_PROTECT	This objective ensures that those responsible for the TOE ensure that the web application has SSL certificates installed and are valid (not revoked or expired) are sourced from a trusted entity.
A.CLOUD	OE.CLOUD	This objective ensures that the cloud environment that the TOE resides provide a load balancing, web application firewall (WAF) and network traffic filters (e.g. access control lists (ACL)) services in order to protect the TOE from any malicious activity and application failure

5 Security requirements

5.1 Overview

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 (REV 5) of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions used within this ST to depict their application:

- **Assignment.** The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows [**assignment**].

- **Selection.** The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].

- **Refinement.** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions~~.

- **Iteration.** The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows FDP_IFF.1a and FDP_IFF.1b.

5.2 Security functional requirements

5.2.1 Overview

The security functional requirements are expressed using the notation stated in Section 5.1 above and are itemised in the table below.

Identifier	Title
User Data Protection	
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute-based access control
Identification and Authentication	

Identifier	Title
FIA_ATD.1	User Attribute Definition
FIA_SOS.1	Verification of Secrets
FIA_UAU.1	Timing of Authentication
FIA_UAU.2	User authentication before any action
FIA_UAU.6	Re-Authenticating
FIA_UID.2	User identification before any action
Security Management	
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
Protection of the TSF	
FPT_STM.1	Reliable time stamps.

5.2.2 FDP_ACC.1a Subset access control (Admin)

Hierarchical to:	No other components.
FDP_ACC.1.1a	The TSF shall enforce the [**Admin Access Control SFP**] on [**Admins performing the following operation (or management functions) to the user accounts:** **a. User Management: Add User, View/Edit User Profile and Terminate User** **b. Group Management: Add/Edit/Delete Group, Edit User Permission Group, Edit User Group** **c. Organisation: Add/Edit/Delete Job Title** **d. Organisation: Add/Edit/Delete Department** **e. Leave Management** **f. Talent Management** **g. Payroll Management** **h. Benefits Store: Health Benefit Management**

	i. **Edit Office and Time zone setting** j. **Change password for own account**]**.**
Dependencies:	FDP_ACF.1 – Security attribute-based access control
Notes:	None.

5.2.3 FDP_ACC.1b Subset access control (Authorized User)

Hierarchical to:	No other components.
FDP_ACC.1.1b	The TSF shall enforce the [**Authorised User Access Control SFP**] on [Authorised **User performing the following operation (or management functions) to the user accounts:** **a) User Management: View/Edit User Profile** **b) Leave Management** **c) Change password for own account]**
Dependencies:	FDP_ACF.1 – Security attribute-based access control
Notes:	None.

5.2.4 FDP_ACF.1 Security attribute-based access control

Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the [**Access Control SFP]** to objects based on the following: [**usernames, user groups and access control list**].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[users are explicitly granted access to a permission or resource if he/she belongs to a user group which has been granted access].**
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[None].**
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[None].**
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static Attribute initialisation
Notes:	None.

5.2.5 FIA_ATD.1 User attribute definition

Hierarchical to:	No other components

FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [**a. Username,** **b. Password,** **c. User group or permission,** **d. Role**].
Dependencies:	No dependencies
Notes:	None.

5.2.6 FIA_SOS.1 Verification of secrets

Hierarchical to:	No other components.
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet [**a minimum password length of 8-characters with at least 1 capital letter and 1 special or numeric character**]
Dependencies:	No dependencies
Notes:	None.

5.2.7 FIA_UAU.1 Timing of authentication

Hierarchical to:	No other components.
FIA_UAU.1.1	The TSF shall allow [**initiation of the change password feature, initiation of the activate account]** on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

5.2.8 FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication
FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

5.2.9 FIA_UAU.6 Re-authenticating

Hierarchical to:	No other components.
FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions [**no user interaction has been detected over 30 minutes**].
Dependencies:	No dependencies
Notes:	None.

5.2.10 FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	No dependencies.
Notes:	None.

5.2.11 FMT_MSA.1 Management of security attributes

Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the [**Access Control SFP**] to restrict the ability to [***modify***] the security attributes [**users permission group]** to [**Admin**].
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.12 FMT_MSA.3 Static attribute initialisation

Hierarchical to:	No other components
FMT_MSA.3.1	The TSF shall enforce the [**Access Control SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP
FMT_MSA.3.2	The TSF shall allow the [**none**] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes

	FMT_SMR.1 Security roles
Notes:	None.

5.2.13 FMT_MTD.1 Management of TSF data

Hierarchical to:	No other components
FMT_MTD.1.1	The TSF shall restrict the ability to [***change***] the [**User Password/Admin Password**] to [**Authorised User and Admin**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.14 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: **[Refer to Table 1 below].**
Dependencies:	No dependencies.
Notes:	**Table 1 - List of Management Function**

User Role	Management Function
Admin	a) User Management: Add User, View/Edit User Profile and Terminate User b) Group Management: Add/Edit/Delete Group, Edit User Permission Group, Edit User Group c) Organisation: Add/Edit/Delete Job Title d) Organisation: Add/Edit/Delete Department e) Leave Management f) Talent Management g) Payroll Management h) Benefits Store: Health Benefit Management i) Edit Office and Time zone setting j) Change password for own account
Authorised User	a) User Management: View/Edit User Profile b) Leave Management c) Change password for own account

5.2.15 FMT_SMR.1 Security Roles

Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles [**Authorised User and Admin**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

5.2.16 FPT_STM.1 Reliable Time Stamps

Hierarchical to:	No other components.
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps.
Dependencies:	No dependencies
Notes:	None.

5.3 TOE Security assurance requirements

EAL2 requires evidence relating to the design information and test results, but does not demand more effort on the part of the developer than is consistent with good commercial practice.

EAL2 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation and a basic description on the architecture of the TOE, to understand the security behaviours.

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to attackers with basic attack potential.

EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification

Assurance class	Assurance components
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_CMC.2 Use of a CM system
	ALC_DEL.1 Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security Problem Definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.2 Independent testing - sample
	ATE_FUN.1 Functional testing
	ATE_COV.1 Evidence of coverage
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

5.4 Security requirements rationale

5.4.1 Dependency rationale

The table below demonstrates the mutual supportiveness of the SFRs for the TOE by demonstrating how the SFR dependencies are fulfilled by the TOE and by justifying those dependencies that are not fulfilled.

The SARs relevant to the TOE constitute an evaluation assurance level of EAL2, as defined in the Common Criteria and include no extensions or augmentations. Therefore, as a complete evaluation assurance level, they are a mutually supportive set and require no further justification.

SFR	Dependency	Inclusion
FDP_ACC.1	FDP_ACF.1 Security attribute-based access control	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static Attribute initialisation	FDP_ACC.1 FMT_MSA.3
FIA_ATD.1	No dependencies	N/A
FIA_SOS.1	No dependencies	N/A
FIA_UAU.1	FIA_UID.1 Timing of identification	FIA_UID.2
FIA_UAU.2	FIA_UID.1 Timing of identification	FIA_UID.2
FIA_UAU.6	No dependencies	N/A
FIA_UID.2	No dependencies	N/A
FMT_MSA.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 FMT_SMR.1
FMT_MTD.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 FMT_SMR.1
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.2
FPT_STM.1	No dependencies	N/A

5.4.2 Mapping of SFRs to security objectives for the TOE

Security objective	Mapped SFRs	Rationale
O.ACC_CONTROL	FDP_ACC.1	The requirement helps meet the objective by identifying the objects and users subjected to the access control policy.
	FDP_ACF.1	The requirement meets the objective by ensuring the TOE only allows access to objects based on the defined access control policy.

Security objective	Mapped SFRs	Rationale
O.AUTH	FIA_UAU.1	The requirement helps meet the objective by allowing the users to change password and activate account before the user is authenticated. It also helps meet the objective by authenticating the users before any TSF mediated actions.
	FIA_ATD.1	The requirement helps meet the objective by maintaining the usernames and passwords, user group and role.
	FIA_UAU.2	The requirement helps meet the objective by authenticating the users before any TSF mediated actions.
	FIA_UAU.6	The requirement helps meet the objective by re-authenticating the users after 30 minutes inactive user interaction.
	FIA_UID.2	The requirement helps meet the objective by identifying the users before any TSF mediated actions.
O.MANAGE	FMT_MSA.1	The requirement helps meet the objective by restricting the ability to modify user permission group to Authorised User and Admin
	FMT_MSA.3	The requirement helps meet the objective by restricting access to provide default values for security attributes that are used to enforce the SFP
	FMT_MTD.1	The requirement helps meet the objective by allowing only users/authorised user and admin to change user password/admin password
	FMT_SMF.1	The requirement helps meet the objective by specifying the management functions of the TOE. Refer to Table 1 for list of management function.
	FMT_SMR.1	The requirement helps meet the objective by maintaining Admin and manages multiple user roles.
	FPT_STM.1	The requirement helps meet the objective by providing reliable time stamps.
O.PASSWORD	FIA_SOS.1	The requirement helps meet the objective by providing a minimum password length of 8-characters with at least 1 capital letter and 1 special or numeric character.

5.4.3 Explanation for selecting the SARs

The assurance package for the evaluation of the TOE is Evaluation Assurance Level 2 (EAL2).

The TOE has a low to moderate level of assurance in enforcing its security functions when instantiated in its intended environment, which imposes no restrictions on assumed activity on applicable networks. EAL2 is sufficient to demonstrate that the TOE is resistant to attackers with a Basic attack potential.

6 TOE summary specification

6.1 Overview

This section provides the TOE summary specification, a high-level description of how the TOE actually implements the claimed security functional requirements.

The TOE security functions include the following:

- **Access Control**
- **Identification and Authentication**
- **Security Management**

6.2 Access Control

The TOE enforces an access control policy on protected resources. After a user is identified and authenticated to the TOE, the TOE will check all HTTP requests from the user to the protected resource. The TOE will permit a user to access a protected resource only if a user ID or role has permission to perform the requested action on the resource (**FDP_ACC.1, FDP_ACF.1**). The TOE maintains access control lists (ACL) for each object within an organisation. Each ACL maps users and roles to the operations that they are permitted to perform on the object.

There are two (2) user roles maintained by the TOE. They are Authorised Users and Admins (**FMT_SMR.1**). Each type of user will have different permission to a protected resource. All users will have a unique user ID. Admin user is the only user that has the ability to assign privilege to each individual Authorised User.

6.3 Identification and Authentication

When a user issues a request to the TOE to access a protected resource, the TOE requires that the user (Authorised User and Admin) to identify and authenticate themselves before performing any TSF mediated action (**FIA_UAU.1, FIA_UAU.2, FIA_UID.2,**). In order for the users to access the TOE, users need to browse to https://www.swingvy.com and click on the 'Login' menu. At the login page, users need to key in a valid username and password in order to access the TOE (**FIA_ATD.1**). The acceptable minimum password length is 8-characters with at least 1 capital letter and 1 special or numeric character. The TOE checks the credentials presented by the user against the authentication information stored in the database and grant access if they are match.

Under the conditions where no user interaction has been detected over 30 minutes, user has to re-authenticate **(FIA_UAU.6**). The TOE compares the credentials by checking the information presented by the user at the login page against the authentication information stored in the database.

All user presented passwords are hashed before being used to authenticate to the TOE, or when users change their passwords (**FMT_MTD.1, FIA_SOS.1**) to be written to the database. This is all done by the TOE

6.4 Security Management

The TOE contains various management functions to ensure efficient and secure management of the TOE (**FMT_SMF.1, FMT_MSA.3**):

Admin role can modify the access control list and mapping of users to roles (**FMT_MSA.1**). TOE provides a suite of management functions to Admin and Authorised User. These functions allow for the configuration of the TOE to suit the organization in which it is deployed. Additionally, management roles may perform the following tasks:

a) Admin User:

- User Management: Add User, View/Edit User Profile and Terminate User
- Group Management: Add/Edit/Delete Group, Edit User Permission Group, Edit User Group
- Organisation: Add/Edit/Delete Job Title
- Organisation: Add/Edit/Delete Department
- Leave Management
- Talent Management
- Payroll Management
- Benefits Store: Health Benefit Management
- Edit Office and Time zone setting (**FPT_STM.1**)
- Change password for own account (**FIA_SOS.1, FMT_MTD.1**)

b) Authorised User:

- User Management: View/Edit User Profile
- Leave Management
- Change password for own account (**FIA_SOS.1, FMT_MTD.1**)

Admin may assign and adjust the functions available to authorised user and adjust the functions based on organization's requirement(s) (**FMT_SMR.1**).